Enterprise ROPA and Data Mapping

BDC-OPS-004 | Consolidated case study v1.1 | 15 November 2026

Prepared by Olumuyiwa Michael, CIPP/US, CIPP/E, CIPM, AIGP, CompTIA Security+

Published by BloomDale Capital LLC • Fictional enterprise: Meridian Digital Holdings • Scope: Article 30 records of processing, enterprise data map, transfers, retention and record quality

SIMULATION DISCLOSURE Meridian Digital Holdings, its systems, vendors, agreements, records and findings are fictional. Nothing here describes a real organization or is legal advice. Legal references were reviewed as of 15 November 2026.

1. Executive brief

Status: baseline not yet approved. Meridian now has one record of processing covering all 16 activities across its four business units and corporate functions, linked to 20 systems, 20 vendors and 21 data flows. It closes the gap behind BDC-PRIV-001 finding GC-F01 (Incomplete ROPA / lawful basis, 16 High), whose evidence was that marketing and analytics flows were missing. Those flows are now ROPA-007 and ROPA-016, and all six AI systems in Meridian's inventory are tied to the activities that use them.

Seven records are ready for owner and Legal sign-off. Nine are blocked: seven by a Critical or High risk, and two by a gap visible in the record itself. The four Critical risks are a marketing pixel and a missing subcontractor BAA on the HealthTech portal, the credit model's missing evidence, and unverified consent and withdrawal for the AI-06 personalization platform.

Measure, 15 November 2026	Current state
Processing activities recorded	16 (Article 30(1) fields complete)
Records approved	0 of 16
Ready for owner approval / blocked	7 / 9
Systems, vendors, data flows	20, 20, 21
AI systems mapped to activities	6 of 6 (AI-01 to AI-06)
Quality checks (8 per record)	128: 103 met, 9 gaps, 16 awaiting approval
Open risks	14: 4 Critical, 4 High, 6 Moderate
Flows with a missing safeguard	1 (FLOW-09, AtlasSupport onward transfer)

2. How the record is built

Each activity is recorded once, with the purpose, people, data, systems, recipients, transfers, retention and safeguards that Article 30(1) requires. U.S. state treatment, sector law, AI systems and links to other portfolio documents sit alongside. Records are written for the business: one row per thing Meridian does with personal data, not per system or per vendor.

Article 30 header	Entry
Controller	Meridian Digital Holdings, Inc. (fictional), U.S.-headquartered group; no establishment in the EU or UK
GDPR scope	EU GDPR and UK GDPR Article 3(2): Digital Learning and Digital Platforms offer services to, and monitor, people in the EU and UK (BDC-PRIV-001)
EU representative (Art 27)	Meridian EU Representation Ltd (fictional), Dublin, Ireland; eu-rep@meridian-demo.invalid. Maintains this record with Meridian (Art 30(1)) and provides it to supervisory authorities on request (Art 30(4))
UK representative (UK GDPR Art 27)	Meridian UK Representation Ltd (fictional), London; uk-rep@meridian-demo.invalid. Maintains the UK-relevant entries
Data protection officer	Data Protection Officer, dpo@meridian-demo.invalid (portfolio assumption: Art 37(1)(b) applies because Digital Platforms monitors EU and UK users regularly, systematically and at large scale)
Processor records (Art 30(2))	Not required: Meridian does not act as a processor for EU or UK controllers. Meridian HealthTech acts as a HIPAA business associate for a U.S. covered entity; that role is recorded in ROPA-003 and governed by the BAA, not Art 30(2)
Article 30(5) exemption	Not available: the processing is not occasional and is likely to result in a risk to individuals (large-scale online monitoring)

The record links to the rest of the portfolio rather than repeating it. BDC-OPS-001 supplies the rights-request process (ROPA-009, ROPA-012), BDC-OPS-002 the AI-06 DPIA (ROPA-002), and BDC-OPS-003 the consent design and tracker inventory (ROPA-006, ROPA-016). Vendors V-101 to V-106 keep the IDs they have in the BDC-PRIV-001 vendor register, so a finding on CareLink Analytics or DecisionPilot AI traces straight to the activities it affects.

3. Enterprise data map

Figure 1 shows who each unit collects data from, the systems that hold it and where it goes. GDPR and UK GDPR reach Meridian only through the Digital Learning and Digital Platforms activities and the corporate functions that support them, such as rights requests and deletion. HealthTech, Financial Services, the workforce and vendor management involve U.S. individuals only or do not engage Article 3(2), which keeps GDPR out of the records where it does not belong.

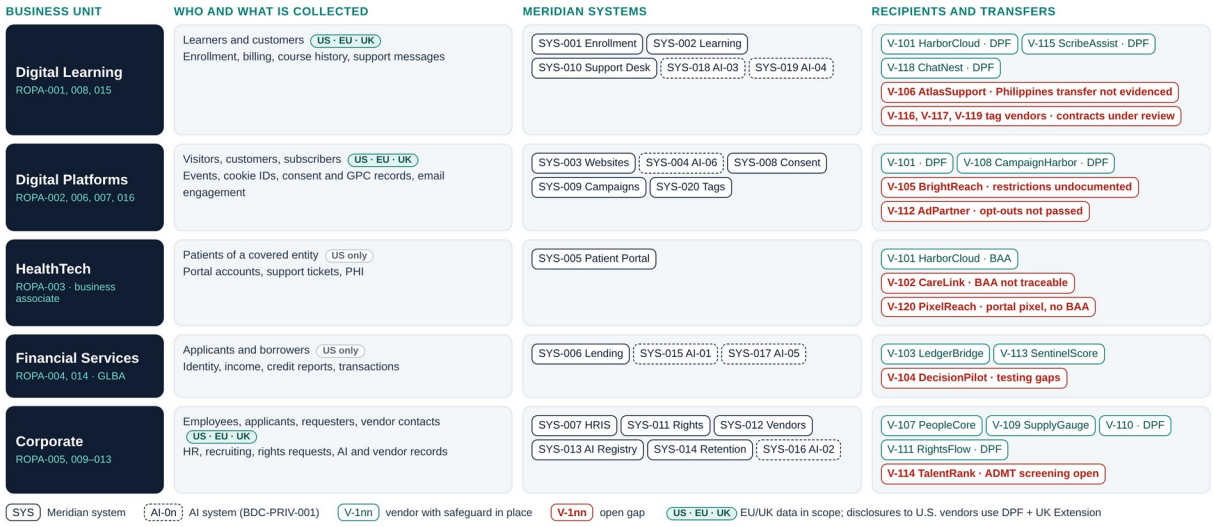


Figure 1. Enterprise data map. Red items have an open gap; dashed items are AI systems. Original illustration.

4. Processing inventory

ID	Activity	Unit	Legal treatment	Status
ROPA-001	Course enrollment and delivery	Digital Learning	Contract, Art 6(1)(b)	Ready for owner approval
ROPA-002	Website personalization (AI-06)	Digital Platforms	Consent for event collection, Art 6(1)(a); legitimate interests for CRM segments, Art 6(1)(f)	Blocked
ROPA-003	Patient portal support	HealthTech	HIPAA Privacy and Security Rules; BAA with covered entity	Blocked
ROPA-004	Consumer loan applications and credit decisions (AI-01)	Financial Services	GLBA Privacy and Safeguards Rules; ECOA / Reg B; FCRA	Blocked
ROPA-005	Employee onboarding and HR administration	Corporate	FLSA, IRCA (Form I-9), state employment law	Ready for owner approval
ROPA-006	Consent and opt-out preference records	Digital Platforms	Legal obligation to demonstrate consent, Art 6(1)(c) with Art 7(1)	Ready for owner approval

ID	Activity	Unit	Legal treatment	Status
ROPA-007	Email marketing and campaigns	Digital Platforms	Consent for new subscribers, Art 6(1)(a) (ePrivacy Art 13(1); PECR reg 22). Existing customers: soft opt-in (ePrivacy Art 13(2); PECR reg 22(3)) on legitimate interests, Art 6(1)(f)	Blocked
ROPA-008	Customer support and AI support assistant (AI-04)	Digital Learning	Contract, Art 6(1)(b); legitimate interests for AI summaries, Art 6(1)(f)	Blocked
ROPA-009	Privacy rights requests (BDC-OPS-001)	Corporate	Legal obligation, Art 6(1)(c) (Arts 12-23)	Ready for owner approval
ROPA-010	Vendor due diligence and monitoring	Corporate	B2B contact data: CT and TX exclude; CCPA B2B exemption expired 1 Jan 2023	Ready for owner approval
ROPA-011	AI governance records	Corporate	Legitimate interests, Art 6(1)(f)	Ready for owner approval
ROPA-012	Retention, deletion and suppression	Corporate	Legal obligation, Art 6(1)(c) (Arts 5(1)(e), 17)	Blocked
ROPA-013	Recruiting and applicant ranking (AI-02)	Corporate	Title VII, FEHA	Blocked
ROPA-014	Transaction fraud detection (AI-05)	Financial Services	GLBA Safeguards Rule	Blocked
ROPA-015	Learning recommendations (AI-03)	Digital Learning	Legitimate interests, Art 6(1)(f), with right to object	Ready for owner approval
ROPA-016	Site analytics and targeted advertising	Digital Platforms	Consent, Art 6(1)(a) with ePrivacy Art 5(3) / PECR reg 6. UK first-party statistics (TRK-003) run under the PECR statistics exception on legitimate interests, Art 6(1)(f), with an opt-out	Blocked

5. Legal treatment

Where the portfolio has already settled a legal question, the record states the answer rather than marking it for review.

Area	Treatment in the record
GDPR and UK GDPR	Apply under Article 3(2) to Digital Learning and Digital Platforms only. Lawful bases are recorded per purpose: contract for enrollment and support, consent for website events, advertising and EU/UK email marketing, legitimate interests for CRM segments and on-platform recommendations (with the right to object).

Area	Treatment in the record
HIPAA	Meridian HealthTech is a business associate of a U.S. covered entity (ROPA-003). Retention follows the covered entity's BAA, with PHI returned or destroyed at termination; patient requests are referred to the covered entity. HarborCloud, which hosts the portal, works under a subcontractor BAA. Texas and Connecticut exempt HealthTech as a business associate, and the CCPA exempts PHI. GDPR does not apply.
GLBA, ECOA and FCRA	Meridian Financial Services is a GLBA financial institution (ROPA-004, ROPA-014). GLBA data is exempt at data level under the CCPA and the CTDPA, and Texas exempts the entity. Since 1 July 2026, Connecticut no longer exempts non-bank lenders as entities (SB 1295), so Financial Services data outside GLBA, such as website and marketing data, is in CTDPA scope. Credit application records are kept 25 months under Regulation B.
California workforce data	The CCPA has covered employee, applicant and B2B contact data since 1 January 2023, when the temporary exemptions expired. ROPA-005, ROPA-010 and ROPA-013 record this; Connecticut and Texas still exclude employment data.
AI systems	Each AI system sits inside the activity that uses it: AI-01 credit decisions (ROPA-004), AI-02 applicant ranking (ROPA-013), AI-03 learning recommendations (ROPA-015), AI-04 support summaries (ROPA-008), AI-05 fraud detection (ROPA-014), AI-06 personalization (ROPA-002). Applicant ranking is flagged for screening against the California ADMT requirements, which apply from 1 January 2027.

6. International transfers

Meridian is a U.S. company with no EU or UK establishment. When EU or UK users give Meridian their data directly, that collection is not a transfer under EDPB Guidelines 05/2021. Meridian is still subject to GDPR for that data under Article 3(2), so when it passes the data to a vendor outside the EEA or UK, the EDPB treats that disclosure as a transfer that needs a tool. The record applies this to every vendor:

- Twelve vendors receive EU or UK personal data. All twelve are certified under the EU-U.S. Data Privacy Framework and its UK Extension, with standard contractual clauses kept ready as a fallback.
- **Gap:** AtlasSupport Global (V-106) is certified, but its agents in a Philippines support center open EU and UK tickets. That is an onward transfer by AtlasSupport, which the DPF onward-transfer principle requires it to cover by contract. Meridian has no evidence of that contract or of a transfer risk assessment (FLOW-09, risk RK-06, High).
- CampaignHarbor (V-108) receives data in the U.S. under its DPF certification. Its email delivery sub-processor is in Ireland, inside the EU, so that leg is not a transfer at all.
- Vendor due diligence (ROPA-010) is outside GDPR: buying from EU or UK suppliers is neither offering them services nor monitoring them, so Article 3(2) is not engaged.

7. Retention schedule

Every record states a retention period and its basis. Where a law sets the period, the record cites it; otherwise the period is labeled as a Meridian policy choice.

Record type	Period	Basis
Privacy request records	24 months	CCPA regulations §7101(a)

Record type	Period	Basis
Consumer credit applications	25 months after notice of action	Regulation B, 12 CFR 1002.12(b)
Applicant and personnel files (California)	4 years from creation, and for applicants and former employees 4 years from the hiring decision or termination	Cal. Gov. Code §12946
Form I-9	3 years after hire or 1 year after termination, whichever is later	IRCA; 8 CFR 274a.2
HIPAA policies and documentation	6 years	45 CFR 164.316(b)(2)
PHI held for the covered entity	Per BAA; return or destroy at termination	45 CFR 164.504(e)
AI-06 raw events / derived features	90 days / 12 months	BDC-OPS-002 PBD-02, PBD-07
Support cases, campaign engagement	24 months	Meridian policy
Analytics and ad identifiers	Up to 13 months	BDC-OPS-003 tracker inventory

8. Where rights requests must reach

The DSAR search map lists, for each system, the key used to find a person, which request types apply and what may be kept after deletion. It gives BDC-OPS-001 a defined search scope. Examples of the exceptions it records:

System	Search key	What deletion does not remove
SYS-005	Not searched by Meridian	Requests go to the covered entity under the BAA
SYS-006	SSN last 4 + name; loan ID	GLBA and Reg B 25-month retention
SYS-008	Cookie ID; customer ID	Opt-out records kept to honor the opt-out
SYS-009	Email	Hashed suppression entry kept
SYS-011	Request ID	Request log kept 24 months (§7101)
SYS-016	Email; applicant ID	FEHA 4 years
SYS-020	Cookie ID (via vendor)	None

9. Risks and actions

Risks and remediation now sit in one register. Scores use the portfolio bands (Low 1–5, Moderate 6–12, High 13–19, Critical 20–25); risks carried from an earlier finding keep that finding's score.

ID	Risk	Record	Score	Source
RK-01	Third-party pixel (TRK-012) on authenticated portal pages discloses PHI to a vendor with no BAA	ROPA-003	4 × 5 = 20 Critical	BDC-OPS-003 R09
RK-02	CareLink Analytics receives PHI with no traceable subcontractor BAA	ROPA-003	4 × 5 = 20 Critical	BDC-PRIV-001 TP-F01
RK-03	DecisionPilot credit model lacks lineage, testing and human-review evidence	ROPA-004	4 × 5 = 20 Critical	BDC-PRIV-001 TP-F02
RK-04	AI-06 event collection and withdrawal not verified end to end	ROPA-002	4 × 5 = 20 Critical	BDC-OPS-002 R01; PBD-01, PBD-04
RK-05	Opt-outs not passed to AdPartner and BrightReach	ROPA-016	4 × 4 = 16 High	BDC-PRIV-001 US-F01 / GC-F02; BDC-OPS-003 R03
RK-06	AtlasSupport's onward transfer of EU and UK tickets to its Philippines center is not evidenced	ROPA-008	4 × 4 = 16 High	New in BDC-OPS-004
RK-07	Applicant ranking (AI-02) not screened for California ADMT requirements that apply from 1 Jan 2027; vendor contract lacks bias-testing terms	ROPA-013	4 × 4 = 16 High	BDC-PRIV-001 AI module
RK-08	Deletion and opt-out instructions not confirmed by downstream vendors	ROPA-012	4 × 4 = 16 High	BDC-OPS-001 deletion workflow
RK-09	BrightReach treated as service provider without contract restrictions	ROPA-007	3 × 4 = 12 Moderate	BDC-PRIV-001 TP-F05
RK-10	Support tickets and AI-04 summaries may hold unrequested sensitive data	ROPA-008	3 × 4 = 12 Moderate	New in BDC-OPS-004
RK-11	California employee and applicant notices predate CCPA coverage of workforce data	ROPA-005	3 × 4 = 12 Moderate	New in BDC-OPS-004
RK-12	Identity documents kept with request records beyond verification	ROPA-009	3 × 3 = 9 Moderate	BDC-OPS-001
RK-13	Fraud model (AI-05) has no completed impact assessment	ROPA-014	3 × 4 = 12 Moderate	BDC-PRIV-001 AI module
RK-14	Tag vendors V-116, V-117 and V-119 lack reviewed contracts	ROPA-016	3 × 4 = 12 Moderate	BDC-OPS-003 tracker inventory

10. Record quality and approval

Eight checks run against every record, one per control (RC-01 to RC-08). A check is "met" when the record holds a complete entry, which says nothing yet about whether the underlying control works. Of 128 checks, 103 are met, 16 await owner and Legal approval, and 9 show a gap in the record itself: five records send data to one of eight vendors with a known agreement problem, three AI impact assessments are still open, and one onward transfer is not evidenced. Every gap is also logged as a risk, so nothing blocking approval sits outside the risk register.

Control	Name	Requirement
RC-01	Owner and review date	Every record has a named owner and a review date within 12 months
RC-02	Article 30 completeness	All Art 30(1) fields filled, or marked not applicable with a reason
RC-03	Flow linkage	Every record links to at least one FLOW ID and every flow to a record
RC-04	Vendor reconciliation	Every recipient exists in the vendor register with a role and agreement status
RC-05	Transfer assessment	Every EU/UK disclosure outside the EEA/UK names a transfer tool
RC-06	Retention and disposal	Every record states a retention period and its basis
RC-07	Assessment screening	Every record states a DPIA, HIPAA or AI assessment result
RC-08	Change and approval history	Material changes trigger review; approvals are logged with date and approver

The companion operating procedure (BDC-OPS-004 SOP v1.1) sets out how records are created, reviewed and kept current: nine steps from intake to escalation, with change triggers, roles and target KPIs for coverage, completeness and attestation.

11. Next steps

1. Remove the TRK-012 pixel from the patient portal and locate or execute the CareLink subcontractor BAA (RK-01, RK-02).
2. Finish the AI-06 consent and withdrawal tests that BDC-OPS-002 requires before launch (RK-04).
3. Obtain AtlasSupport's onward-transfer contract and transfer risk assessment for its Philippines center, and restrict that access until then (RK-06).
4. Complete the open AI impact assessments for AI-01, AI-02 and AI-05, starting with California ADMT screening for applicant ranking (RK-03, RK-07, RK-13).
5. Get owner and Legal sign-off on the seven ready records, then run the first annual review by November 2027.

12. Limitations

- All records, agreements and statuses are synthetic. "Met" describes record content, not tested controls.
- Meridian's own disclosures to U.S. vendors are treated as transfers, following the EDPB's reading of Article 3(2) and Chapter V. Some practitioners read this differently; the conservative view is used here.
- DPO designation, representative details and all vendor names are portfolio assumptions.
- Legal conclusions are for a fictional company and would be confirmed by counsel for a real one.

13. Package contents

File	Purpose
BDC-OPS-004_Consolidated_ROPA_Case_Study_v1.1 (.docx, .pdf)	This document
BDC-OPS-004_ROPA_Operating_Procedure_v1.1 (.docx, .pdf)	How records are created, reviewed and maintained
BDC-OPS-004_Enterprise_ROPA_Workbook_v1.1.xlsx	Controller header, ROPA register, systems, vendors, flows, DSAR map, tracker map, risks, quality checks, controls, method
BDC-OPS-004_Executive_Dashboard_v1.1.pptx	Seven-slide management summary with data map

Sources

- GDPR Article 30 (Regulation (EU) 2016/679): https://eur-lex.europa.eu/eli/reg/2016/679/oj
- EDPB Guidelines 05/2021 on Article 3 and Chapter V: https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf
- CCPA regulations effective 1 January 2026 (CPPA): https://cppa.ca.gov/regulations/pdf/ccpa_statute_eff_20260101.pdf
- Regulation B record retention, 12 CFR 1002.12: https://www.consumerfinance.gov/rules-policy/regulations/1002/12/
- California Government Code §12946: https://california.public.law/codes/government_code_section_12946
- UK GDPR Article 30: https://www.legislation.gov.uk/eur/2016/679/article/30
- HIPAA documentation retention, 45 CFR 164.316: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.316
- Form I-9 retention, 8 CFR 274a.2: https://www.ecfr.gov/current/title-8/chapter-I/subchapter-B/part-274a/subpart-A/section-274a.2
- Connecticut Data Privacy Act as amended (ch. 743jj): https://prdext3.cga.ct.gov/2026/sup/chap_743jj.htm
- EU-U.S. Data Privacy Framework program: https://www.dataprivacyframework.gov/

About the author

Olumuyiwa Michael, CIPP/US, CIPP/E, CIPM, AIGP, CompTIA Security+

Privacy and compliance professional with more than seven years of experience in privacy operations, privacy impact assessments, data subject rights, incident management and regulatory compliance, and a technical background in database administration and information security.